Cellebrite
ENDPOINT
INSPECTOR

Communication and Security

September 2021 | Version 1.2

Cellebrite

This page intentionally left blank.

Components

This document explains the design considerations regarding the security of customers' systems and data when using Endpoint Inspector in their infrastructure.

Endpoint Inspector allows an organization to create logical data collections from physically distant computers and mobile devices without shipping any hardware. Endpoint Inspector is made up of these components.

Component	Description
Endpoint server	Installed on a single Windows computer. Servers for Endpoint Inspector are not aware of each other. The Endpoint portal lets administrators log in to the server from a web browser to manage the server, agents and users. In the Endpoint server, examiners can create and manage data collection jobs for mobile agents.
Endpoint agent	Installed on Windows and Mac computers to allow examiners to collect data. When these computers are running and connected to the network, they establish a connection to the Endpoint server and actively await instructions. Collection over a VPN is supported.
Endpoint mobile agent	An examiner provides a download link and instructions to the custodian of an iOS device and may create a password to protect each data collection. The custodian downloads and installs the lightweight Endpoint mobile agent on their Windows computer and follows simple instructions to enable data to be collected from the iOS device in their custody. The Endpoint mobile agent automatically transfers collected data to the shared network location specified by the examiner, and then deletes the collection from the custodian's computer. For examination, the data collection can be ingested into Endpoint Inspector 10.4.1 and later or Physical Analyzer 7.47 and later. Note: Only Windows computers and iOS devices are supported.
Endpoint Inspector	Installed on Windows or Mac computers. Once an examiner selects and connects to an agent, they can collect and examine data from that remote computer. Examiners can also ingest and examine data collected from mobile devices. CPU resources may be consumed from both the examiner's computer and the remote computer, and on rare occasions from the Endpoint server as well.

Network and Application Security

All communication among components of Endpoint is encrypted with TLS 1.3 using both server and client certificate validation. Digital signatures and expiration dates are enforced, and connection attempts can be logged and audited. (Centralized logging and auditing features are not currently implemented.)

Each instance of the Endpoint server can be either self-hosted or run in the cloud. Endpoint agents connect to and maintain a persistent connection with the Endpoint server. Users of Endpoint Inspector authenticate and connect to the Endpoint server to interact with Endpoint agents.

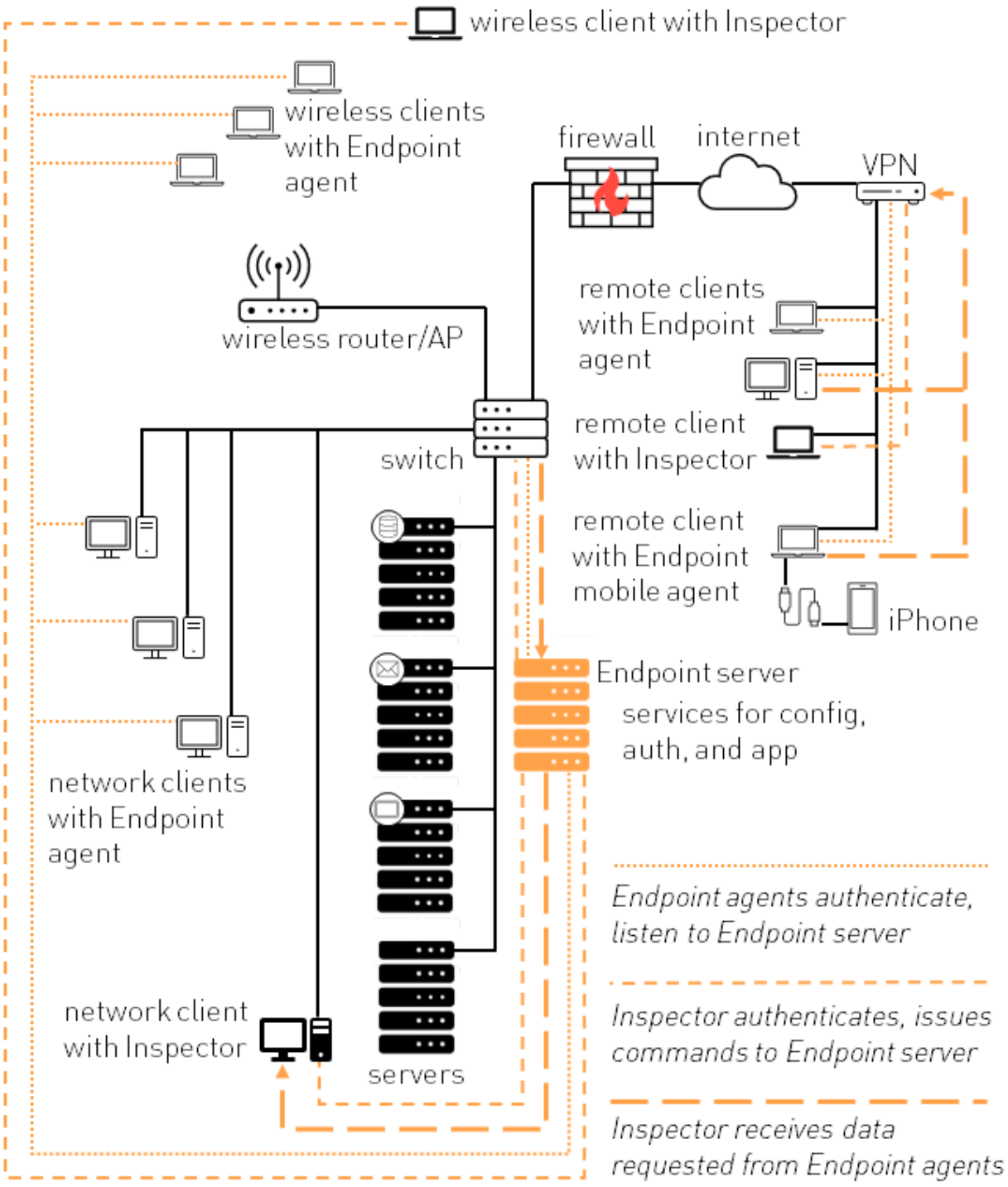
Ports, Services, and Processes

While the Endpoint server is packaged as a single server, it runs three different services listening on their own ports. This modular approach simplifies development and security.

Configuration service port 443	Administrators interact with the configuration service through an HTTPS connection and a web browser. The configuration service is responsible for updating licensing, for adding and managing users and agents, and for viewing the status of the system. Administrators with limited access are prevented from performing certain actions.
Authentication service port 20001	The authentication service is responsible for securely authenticating users and Endpoint agents before they are allowed to connect to the application service. It accomplishes this by issuing signed TLS client certificates after a challenge-response protocol is successful.
Application service port 20002	The application service acts as a proxy to connect authenticated users and Endpoint agents, facilitating requests and responses over a secure channel. The application service rejects all connections for Endpoint agents and users that are not successfully authenticated by the authentication service. It also enforces licensing limitations for maximum concurrent users and Endpoint agents.
Internal communications for mobile agent port 7681	The Endpoint mobile agent runs two separate processes, one for the web browser-based interface that the custodian uses, and one for the back end. The processes use internal communication to interact with each other. The default port is 7681. If the port is already assigned, the agent assigns the next available port within a range of up to 15 ports.

Endpoint Inspector Communications

This diagram represents a simplified enterprise network topology overlaid by Endpoint components and communication pathways.



Troubleshooting

Take these actions to troubleshoot problems with communications among Endpoint components.

1. Verify that ports are open and listening.

    a. Verify that the server and the agents are running.
    Look for running processes with Activity Monitor on macOS or Task Manager on Windows, and then verify that agents and server are running.

    b. Verify that ports are listening.
    Check terminal using netstat to verify that the required ports are listening.

2. Verify that firewalls are not blocking the required ports.

3. Validate that all traffic can connect and that any Network Address Translation (NAT) is working with proper port forwarding.

4. Verify that security protocols are not blocking connections.

5. If you encounter issues collecting from mobile devices, take these actions.

    a. Verify that after the Endpoint mobile agent is started on a custodian's computer, no other USB connections are made until the collection process is complete and the mobile agent is closed.

    b. Because the Endpoint mobile agent uses the iTunes backup protocol for collecting data, the custodian is prompted to enter their backup password. If the custodian does not have a backup password for iTunes, the default password (1234) is used and removed when the collection process is complete. If the collection process is interrupted, this temporary default password is not removed.